Description

Méthode d'allocation de ressources sécurisées dans un module de sécurité

[001] La présente invention concerne le domaine de la téléphonie sans-fil dite aussi téléphonie cellulaire. Elle concerne plus particulièrement des fonctions évoluées impliquant des mécanismes de sécurité ouverts à des fournisseurs spécifiques d'application.

[002] Le module de sécurité d'un téléphone portable, plus connu sous l'appellation "carte SIM", est le cœur de la sécurité de ces téléphones. L'opérateur de téléphonie introduit à la fabrication ou lors d'une phase de personnalisation les informations nécessaires pour identifier d'une manière sûre tous les téléphones voulant se connecter sur son réseau.

[003] A cet effet, il comprend au minimum un numéro unique et une clé cryptographique permettant d'identifier la carte SIM de manière sûre.

[004] Si cette carte était initialement uniquement dédiée au service de téléphonie, de nouvelles applications ont vu le jour telles que l'affichage de cours boursiers ou des informations météo.

[005] Pour parvenir à ce type d'application, le premier modèle a été de relier le fournisseur de ces données à l'opérateur qui les transmettait à destination des téléphones concernés.

[006] Si cette solution convient bien pour des données généralistes telles que la météo, elle est inappropriée en ce qui concerne des données sensibles telles qu'un relevé bancaire.

[007] Ainsi, ce type de service a buté sur un problème de confidentialité car il n'est pas acceptable que de telles données doivent transiter par l'opérateur de téléphonie mobile.

[008] Une autre approche a été de donner aux fournisseurs les moyens cryptographiques (notamment les clés) pour accéder de façon sécurisée à la carte SIM. Cette approche a buté sur le problème inverse au précédent à savoir la transmission de secret de l'opérateur vers un fournisseur, ce qui n'est pas acceptable pour l'opérateur.

[009] Le document US 6'385'723 décrit une solution de chargement d'applications dans une carte électronique (IC card). La méthode décrite consiste à authentifier les applications à charger par une autorité (Certification Authority) avant de pouvoir charger une telle application dans une carte. Cette méthode bien que garantissant une grande sécurité, n'offre aucune souplesse et fait intervenir l'autorité à chaque changement à effectuer dans l'application.

[010] Le document EP 0 973 135 est également une illustration de l'état de la technique. Une machine spécialisée est seule habilitée à mettre à jour des paramètres de sécurité.

Il s'agit plutôt d'une initialisation d'un module de sécurité effectué hors d'une zone protégée. Aucune indication permettant l'accès ou la résiliation d'applications chargées postérieurement est décrite dans ce document.

[011] Ainsi, le but de la présente invention est de proposer une méthode qui tienne compte des impératifs de sécurité des différents intervenants et permette de proposer le téléchargement et la gestion des applications sécurisées d'une manière décentralisée sur un téléphone portable.

[012] Ce but est atteint par une méthode d'allocation de ressources d'un module de sécurité d'un appareil connecté à un réseau, ce réseau étant administré par un opérateur, lesdites ressources étant utilisées par des fournisseurs d'application, cette méthode consistant dans les étapes suivantes :

[013] - génération d'une paire de clés asymétriques et stockage de la clé privée dans le module de sécurité, la clé publique étant stockée chez l'opérateur,

[014] - introduction d'au moins une clé publique de l'opérateur dans le module de sécurité,

[015] - réception par l'opérateur d'une requête d'un fournisseur, cette requête comprenant au moins la clé publique du fournisseur,

[016] - transmission par l'opérateur d'une instruction de réservation d'une ressource vers le module de sécurité accompagnée par la clé publique du fournisseur,

[017] - transmission par l'opérateur de la clé publique du module de sécurité au fournisseur,

[018] - établissement d'une communication sécurisée entre le fournisseur et le module de sécurité,

[019] - chargement d'une application par le fournisseur dans le module de sécurité.

[020] Cette méthode présente l'avantage d'allouer des ressources d'une manière contrôlée du fait que la réservation, voire le blocage d'une ressource est sous le contrôle de l'opérateur alors que l'exploitation de cette ressource est sous le contrôle du fournisseur, sans que l'opérateur puisse avoir accès aux données échangées.

[021] Une ressource est une zone mémoire d'un module de sécurité dont une partie est constituée par un programme et une autre partie est constituée par des données.

[022] Le processeur du module de sécurité exécute le programme de la ressource d'une manière sécurisée c'est-à-dire que l'exécution ne peut faire appel à des plages de la zone mémoire hors de la zone de la ressource.

[023] Grâce à cette ressource, un fournisseur peut par exemple stocker le numéro de compte bancaire et identifier le titulaire du compte.

[024] Si l'opérateur souhaite résilier une ressource, il est le seul à pouvoir dialoguer avec le module de sécurité au niveau de la gestion des ressources. Le blocage ou la libération d'une ressource provoque la désactivation ou l'effacement de toute la zone mémoire dédiée à cette ressource et en particulier la désactivation ou l'effacement de la

clé publique du fournisseur correspondant.

[025] La disparition physique ou virtuelle de cette clé publique interdit toute nouvelle authentification mutuelle entre le fournisseur et le module de sécurité, et empêche par la même occasion une mise à jour ou un nouveau téléchargement d'application par ce même fournisseur dans cette ressource bloquée ou libérée. La zone des ressources comprend une partie de gestion dans laquelle va se trouver la définition de l'utilisation de chaque zone.

[026] Cette partie de gestion est gérée par l'opérateur. Elle contient l'identifiant du fournisseur, la clé de ce fournisseur et des informations permettant l'adressage de la zone mémoire. Cette partie pourra comprendre également des indications de dates si le fournisseur peut utiliser la ressource durant un temps limité. Passé cette date, la ressource est désactivée ou effacée et en particulier, la clé publique du fournisseur est désactivée ou effacée.

[027] Selon une autre variante, cette partie pourra également comprendre des indications du nombre d'exécutions si le fournisseur et/ou l'utilisateur final peut utiliser la ressource pour un nombre d'exécution limité. Passé ce nombre d'exécution, la ressource est désactivée ou effacée et en particulier, la clé publique du fournisseur est désactivée ou effacée.

[028] L'invention sera mieux comprise grâce à la description détaillée qui va suivre et qui se réfère aux dessins annexés qui sont donnés à titre d'exemple nullement limitatif, à savoir:

[029] - la figure 1 illustre l'étape de personnalisation d'un module de sécurité,

[030] - la figure 2 illustre la transmission entre un fournisseur et un opérateur,

[031] - la figure 3 illustre les échanges de données entre les trois entités,

[032] - la figure 4 illustre un module de sécurité à allocation de ressources.

[033] Selon la figure 1, l'initialisation d'un module de sécurité US-SM est effectuée par une entité PS telle qu'un fabricant de modules de sécurité. Cette entité PS place une clé publique KPuIS qui correspond à l'autorité en charge de la gestion de ces modules, ainsi qu'une clé privée KPrUS propre à ce module de sécurité.

[034] Comme il sera décrit plus bas, d'autres paramètres de personnalisation tels que des données de génération b, M (base et modulo) servant à la génération d'une clé symétrique peuvent également être stockés dans le module de sécurité.

[035] L'entité de personnalisation PS renvoie à l'autorité IS les indications de personnalisation c'est-à-dire, pour un module donné (généralement identifié par une adresse unique ou un identificateur unique), sa clé publique KPuUS. D'autres données telles que les caractéristiques du module, comme sa taille mémoire et ses modules cryptographiques sont également mémorisés par l'autorité.

[036] La figure 2 illustre l'opération de requête par un fournisseur FO d'une ressource

auprès de l'opérateur OP.

[037] Afin de pouvoir accéder aux ressources d'un module de sécurité, un fournisseur FO va, dans une première phase, s'adresser à l'opérateur OP. Le fournisseur FO et l'opérateur OP vont alors se mettre d'accord sur les modalités de leur partenariat. Selon notre exemple, l'opérateur OP va requérir les informations nécessaires auprès de l'autorité IS; l'opérateur OP et l'autorité IS étant deux entités différentes. Dans un autre cas, il est possible que l'opérateur OP comprenne les fonctionnalités de l'autorité IS.

[038] Le fournisseur FO va transmettre entre autre sa clé publique KPuFO à l'opérateur OP et l'informer des caractéristiques de la ressource nécessaire. Les données b, M servant à la génération d'une clé symétrique peuvent également être transmises à ce moment.

[039] La figure 3 illustre trois opérations: SER, RES et ACT.

[040] L'étape de réservation RES consiste à créer une ressource dans un module de sécurité. Un abonné, via son module de sécurité US-SM, peut émettre le souhait auprès de l'opérateur OP de profiter des services proposés par le fournisseur FO. Dans un tel cas, l'opérateur OP récupère la clé publique KPuFO du fournisseur FO et ensuite, va initier une opération de réservation de ressource RSC dans le module de sécurité. L'opérateur dispose d'informations concernant l'utilisation des ressources pour chaque module de sécurité. Il pourra déterminer, en fonction du type de besoin du fournisseur FO, la ressource la plus appropriée, par exemple selon la taille de l'espace mémoire demandé.

[041] L'opérateur envoie une commande de réservation vers le module de sécurité, cette commande étant bien entendu sécurisée par la clé privée KPrOP de l'opérateur. Cette commande va réserver une ressource c'est-à-dire qu'une partie de la zone mémoire va recevoir des données propres à autoriser un dialogue avec un fournisseur. Lors de cette opération, le module de sécurité va recevoir la clé publique KPuFO du fournisseur, clé qui lui permettra d'établir une liaison sécurisée avec ce fournisseur.

[042] Durant cette opération, si l'opérateur ne dispose pas de la clé du module de sécurité, il pourra la requérir auprès de l'autorité IS. Cette requête se fait naturellement d'une manière sécurisée entre ces deux entités.

[043] La seconde étape ACT consiste à communiquer les données d'un abonné ou module de sécurité au fournisseur FO. L'opérateur OP lui communique la clé publique KPuUS et l'identification de la ressource RSC qui lui a été attribuée.

[044] Le fait que la clé publique de chaque module de sécurité soit unique, signifie que l'opérateur OP ou l'autorité IS, une fois le module de sécurité US-SM identifié, va rechercher dans sa base de données la clé publique KPuUS propre à ce module pour la transmettre au fournisseur.

[045] Cette initialisation faite, l'étape SER d'utilisation de ce service peut être activée et

l'utilisateur pourra appeler un numéro spécialisé qui le mettra directement en liaison avec le fournisseur. Celui-ci aura pour première mission de charger son application dans le module de sécurité US-SM, dans la zone mémoire qui lui a été allouée par l'opérateur. Une clé de session KS est générée pour l'échange sécurisé de code et/ou de données.

[046] La figure 4 illustre l'organisation du module de sécurité. Ce dernier est composé d'une unité de traitement CPU, d'une mémoire de travail MEM dans laquelle est stocké le programme d'exploitation du module et une zone de mémoire destinée aux ressources externes. Cette zone dispose d'une première partie dite de définition DEF qui contient les données définissant une ressource RSC1 à RSC4. Dans la pratique, la zone mémoire des ressources n'est pas nécessairement divisée à l'avance. Lorsqu'un fournisseur demande une ressource à l'opérateur, il peut spécifier également la taille de la mémoire nécessaire. Ainsi la zone mémoire des ressources pourra contenir d'autant plus de ressources différentes que chaque ressource utilise peu de mémoire. La partie de définition DEF contiendra les indications de début et de fin de chaque ressource.

[047] A chaque ressource RSC peuvent être associées des informations supplémentaires indiquant p.ex. les droits d'accès à certaines interfaces de programmations (ou librairies) disponibles sur le module de sécurité US-SM telles que des algorithmes cryptographiques ou autres processus de calculation particuliers. De telles informations peuvent être sauvegardées p.ex. dans la zone DEF ou dans la zone RSC respective.

[048] Le module I/O schématise la communication avec l'appareil hôte tel qu'un téléphone portable.

[049] Il existe plusieurs méthodes pour l'établissement d'une connexion sécurisée entre deux entités. Dans le cadre de l'invention, il est prévu d'utiliser une paire de clés asymétriques, l'entité principale disposant de la clé privée et l'entité tierce recevant la clé publique. La clé privée n'est en principe pas envoyée par des moyens de télécommunication mais directement introduite dans le dispositif lors d'une phase d'initialisation sécurisée. La clé publique est envoyée selon les scénarios décrits ci-dessus pour dialoguer avec ce dispositif.

[050] En pratique, l'échange d'une clé publique se fait souvent à l'aide d'un certificat associé à cette clé. Lorsqu'une entité B reçoit la clé publique d'une entité A, cette clé est contenue dans un certificat qui est signé par une autorité à laquelle l'entité A fait confiance, par exemple par l'opérateur. Dans certains cas, il peut arriver que les entités A et B se soient déjà authentifiées au préalable et que le canal à travers lequel ils communiquent soit suffisamment sûr pour qu'ils puissent se transmettre une clé publique sans certificat.

[051] Des clés asymétriques, telles que clés RSA, permettent une authentification des partenaires. Une entité A s'authentifie par une opération utilisant sa propre clé privée

KPrA. Une entité B peut alors vérifier la validité de cette authentification à l'aide de la clé publique correspondante KPuA. Le cryptage basé sur des clés asymétriques est lourd et implique des moyens cryptographiques importants. C'est pourquoi les clés asymétriques sont utilisées généralement pour l'authentification et la génération d'une clé de session symétrique. Il est aussi possible d'utiliser les clés asymétriques pour l'authentification, et utiliser la méthode décrite par Diffie & Hellmann pour la génération d'une clé de session symétrique.

[052] Selon un des modes de réalisation, l'étape de réservation d'une ressource comprend, en plus de l'envoi de la clé publique KPuFO du fournisseur, l'envoi des paramètres Diffie & Hellmann soit le module M et la base b propre à ce fournisseur. Ainsi, lors de l'établissement d'une clé de session entre le fournisseur et un module de sécurité d'un abonné, ces paramètres seront utilisés sans qu'il soit nécessaire de les transmettre à nouveau.

[053] Il est possible d'utiliser la même méthode de Diffie & Hellmann pour générer une clé de session entre le module de sécurité et l'opérateur, l'étape d'initialisation des modules de sécurité pourrait comprendre dans ce cas une étape supplémentaire qui consiste à introduire les paramètres Diffie & Hellmann propre à l'opérateur dans les modules de sécurité.

[054] Selon un premier mode de l'établissement d'une liaison sécurisée, l'échange des données entre les deux dispositifs utilisera la clé publique de l'autre dispositif. Cette manière de procéder a l'avantage que dans le même temps qu'une clé symétrique KS est générée permettant de sécuriser les échanges, l'authentification des partenaires est faite.

[055] Selon un deuxième mode de l'établissement d'une liaison sécurisée, une clé de session est générée d'une manière classique entre les entités A et B sur la base des paramètres Diffie & Hellmann. Une fois cette clé de session établie, une procédure d'authentification mutuelle est initiée. Par exemple, l'entité A peut signer à l'aide de sa clé privée KPrA certaines des valeurs échangées avec B lors de la négociation Diffie & Hellman, et adresser à B la signature ainsi générée. L'entité B peut alors authentifier A en vérifiant la signature à l'aide de la clé KPuA. De manière similaire, l'entité B peut signer à l'aide sa clé privée KPrB certaines des valeurs échangées avec A lors de la négociation Diffie & Hellman, et adresser à A la signature ainsi générée. L'entité A peut alors authentifier B en vérifiant la signature à l'aide la clé KPuB.

[056] Il existe aussi d'autres méthodes pour l'établissement de cette liaison sécurisée par exemple en inversant les deux étapes précédentes, c'est-à-dire d'utiliser la cryptographie à clé publique/privée pour authentifier les deux partenaires et ensuite générer la clé de session.

[057] Dans la pratique, il se peut que diverses entités interviennent dans les différentes

étapes. La génération des clés est confiée à une première autorité qui les communique, du moins la partie privée, à un intégrateur en vue de la personnalisation des modules de sécurité. Il est à noter que cette génération peut s'effectuer directement dans le module de sécurité et que seule la clé publique soit communiquée lors d'une phase d'initialisation, dans un environnement sécurisé.

[058] Cette base de données des clés publiques associées au numéro unique (UA) de chaque module de sécurité peut, soit être gérée par l'opérateur, soit être déléguée à une entité tierce. C'est cette entité qui assurera les fonctions d'allocation de ressources en lieu et place de l'opérateur.

[059] Dans une autre forme de réalisation de l'invention, il est souhaitable que le chargement d'une application puisse s'effectuer d'une manière globale. Du fait que les modules de sécurité utilisent une clé unique par module, une étape intermédiaire est ajoutée lors de la réservation de la ressource. Dans les paramètres transmis par l'opérateur OP vers un module de sécurité, une clé de domaine est ajoutée, clé qui est commune à tous les modules de sécurité pour une application donnée. La définition de la ressource est spécifique à chaque module de sécurité selon sa capacité matérielle, mais une fois définie, elle reçoit un nom logique qui est commun à tous les modules ainsi qu'une clé commune. Le fournisseur FO peut donc télécharger, soit simultanément en mode diffusion son application dans tous les modules connectés, soit par une procédure indépendante du module de sécurité, lors d'un appel de ce module au serveur du fournisseur. Cette clé de domaine DK peut être soit symétrique, soit asymétrique selon l'implémentation de la méthode. Cette clé remplacera la paire de clés publique/privée du module de sécurité lors de l'établissement de la liaison sécurisée.

Revendications

[001] Méthode d'allocation de ressources d'un module de sécurité d'un appareil connecté à un réseau, ce réseau étant administré par une opérateur (OP), lesdites ressources (RSC) étant utilisées par des fournisseurs d'application (FO), cette méthode consistant dans les étapes suivantes :
- génération d'une paire de clés asymétriques et stockage de la clé privée dans le module de sécurité (US-SM), la clé publique (KPuUS) étant stockée chez une autorité (IS),
- introduction d'au moins une clé publique de l'autorité (KPuIS) dans le module de sécurité (US-SM),
- réception par l'opérateur (OP) d'une requête d'un fournisseur (FO) et transmission de cette requête à l'autorité (IS), cette requête comprenant au moins la clé publique du fournisseur (KPuFO),
- transmission par l'opérateur (OP) d'une instruction de réservation d'une ressource (RSC) vers le module de sécurité (US-SM) accompagnée par la clé publique du fournisseur (KPuFO),
- transmission par l'opérateur (OP) de la clé publique (KPuUS) du module de sécurité au fournisseur (FO),
- établissement d'une communication sécurisée entre le fournisseur (FO) et le module de sécurité (US-SM),
- chargement d'une application par le fournisseur (FO) dans le module de sécurité (US-SM).

[002] Méthode d'allocation de ressources selon la revendication 1, caractérisé en ce que la paire de clés asymétriques est générée par le module de sécurité, la clé publique étant alors transmise à l'autorité.

[003] Méthode d'allocation de ressources selon la revendication 1, caractérisé en ce que des paramètres d'initialisation d'une clé de session (M, b) propre à l'opérateur sont stockés dans les modules de sécurité lors de l'initialisation.

[004] Méthode d'allocation de ressources selon les revendications 1 à 3, caractérisée en ce que le fournisseur transmet des paramètres d'initialisation d'une clé de session (M, b) à l'opérateur, ces paramètres étant transmis au module de sécurité lors de la réservation d'une ressource.

[005] Méthode d'allocation de ressources selon les revendications 1 à 4, caractérisée en ce que l'établissement d'une communication sécurisée entre le fournisseur et le module de sécurité est basé sur l'utilisation de la clé publique du fournisseur par le module de sécurité et par l'utilisation de la clé publique du module de sécurité par le fournisseur.

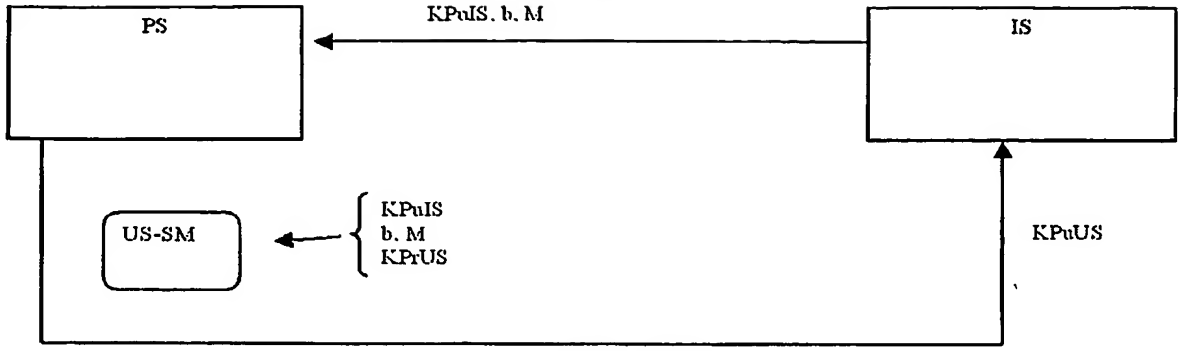
[006] Méthode d'allocation de ressources selon la revendication 3, caractérisée en ce que l'établissement d'une communication sécurisée entre l'opérateur et le module de sécurité est basé sur la génération d'une clé de session utilisant les paramètres d'initialisation (M, b) de l'opérateur.

[007] Méthode d'allocation de ressources selon la revendication 4, caractérisée en ce que l'établissement d'une communication sécurisée entre le fournisseur et le module de sécurité est basé sur la génération d'une clé de session utilisant les paramètres d'initialisation (M, b) du fournisseur.

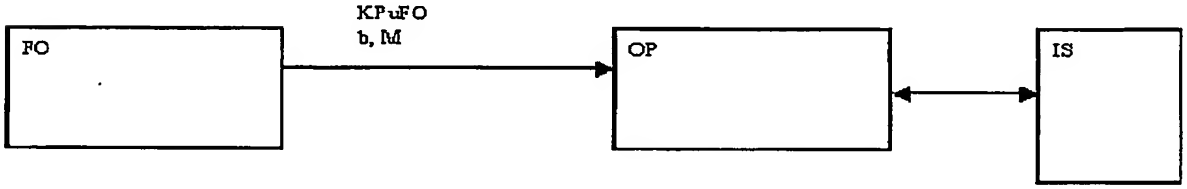
[008] Méthode d'allocation de ressources selon l'une des revendications précédentes, caractérisée en ce que l'autorité (IS) et l'opérateur (OP) forment une même entité.

[009] Méthode d'allocation de ressources selon l'une des revendications précédentes, caractérisée en ce que l'instruction de réservation d'une ressource (RES) comprend l'envoi d'une clé de domaine (DK) spécifique à une application et commune à tous les modules de sécurité disposant de cette application, cette clé étant utilisée pour l'établissement de la communication sécurisée entre le fournisseur FO et le module de sécurité.

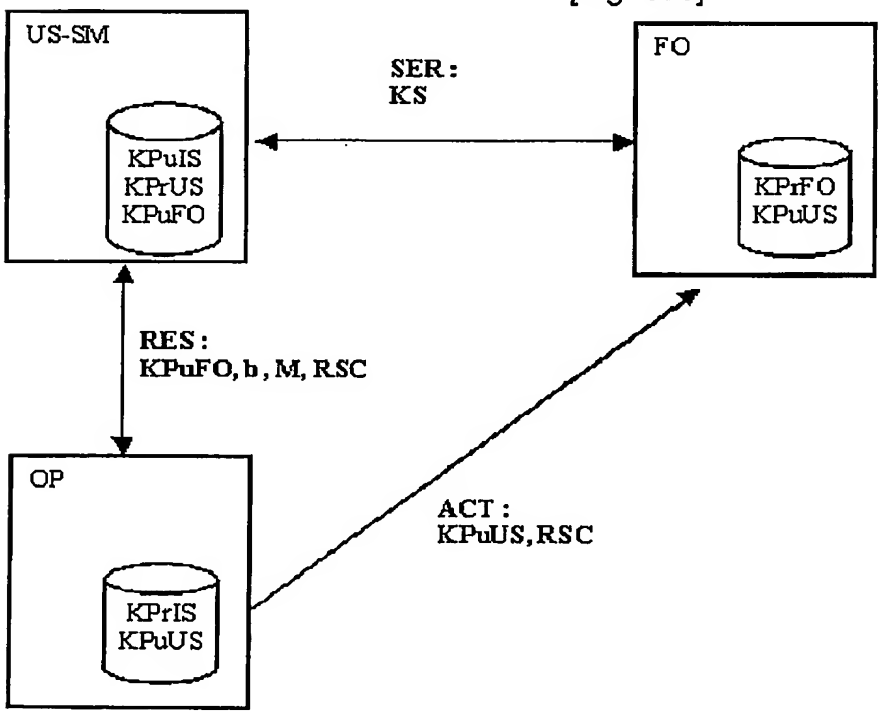
[Fig. 001]



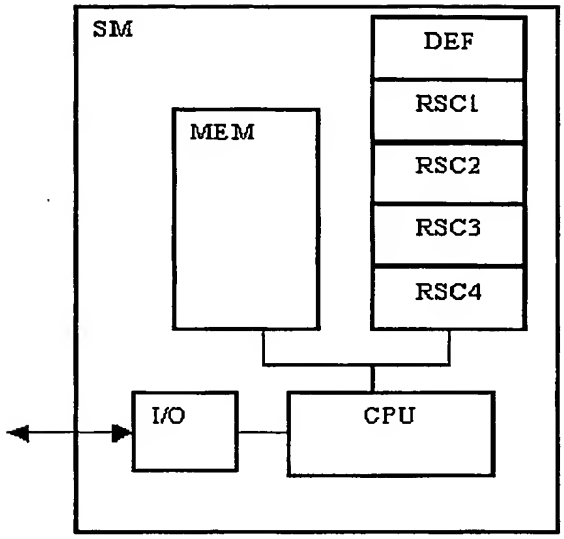
[Fig. 002]



[Fig. 003]



[Fig. 004]



INTERNATIONAL SEARCH REPORT

Internatic... Application No
PCT/EP2004/051198

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6 385 723 B1 (RICHARDS TIMOTHY PHILIP) 7 May 2002 (2002-05-07) column 4, line 10 - column 12, line 16 figure 1 -----	1-9
Y	EP 0 973 135 A (SONY CORP) 19 January 2000 (2000-01-19) column 12, paragraph 78 - column 13, paragraph 87 column 16, paragraph 105 - column 17, paragraph 110 column 19, paragraph 125 - paragraph 126 figure 7 -----	1-9
A	US 5 577 121 A (DAVIS TERRY L ET AL) 19 November 1996 (1996-11-19) abstract -----	2
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 August 2004	30/08/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Rachkov, V

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/051198

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	BRUCE SCHNEIER: "Applied Cryptography" 1996, JOHN WILEY & SONS, INC. , USA 238530 , XP002267052 page 513 - page 514	3,4,6,7
A	WO 01/27886 A (HAEMAELAEINEN ANTTI ;SONERA SMARTTRUST OY (FI)) 19 April 2001 (2001-04-19) page 6, line 1 - page 13, line 7 figure 3	1
A	US 2002/050528 A1 (MILLER STUART JAMES ET AL) 2 May 2002 (2002-05-02) page 1, paragraph 6 page 2, paragraph 25 - page 3, paragraph 32 page 5, paragraph 55 - page 8, paragraph 82 figure 10	1-9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2004/051198

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6385723 B1	07-05-2002	AU 7777098 A	08-12-1998
		EP 0985203 A1	15-03-2000
		WO 9852161 A2	19-11-1998
		JP 2001525957 T	11-12-2001
		AU 736325 B2	26-07-2001
		AU 6299698 A	09-09-1998
		AU 7776798 A	08-12-1998
		AU 7776898 A	08-12-1998
		AU 7776998 A	08-12-1998
		AU 7777198 A	08-12-1998
		AU 7777298 A	08-12-1998
		AU 7777398 A	08-12-1998
		AU 7777498 A	08-12-1998
		CA 2281576 A1	27-08-1998
		DE 69807210 D1	19-09-2002
		DE 69807210 T2	24-04-2003
		DE 69813208 D1	15-05-2003
		DE 69813208 T2	05-02-2004
		DE 69823649 D1	09-06-2004
		EP 0963580 A1	15-12-1999
		EP 0981807 A2	01-03-2000
		EP 0985202 A1	15-03-2000
		EP 0976114 A2	02-02-2000
		EP 0985204 A1	15-03-2000
		EP 0981805 A1	01-03-2000
		WO 9837526 A1	27-08-1998
		WO 9852158 A2	19-11-1998
		WO 9852159 A2	19-11-1998
		WO 9852160 A2	19-11-1998
		WO 9852152 A2	19-11-1998
		WO 9852162 A2	19-11-1998
		WO 9852163 A2	19-11-1998
		WO 9852153 A2	19-11-1998
		HK 1022364 A1	02-05-2003
		JP 2001513231 T	28-08-2001
		JP 2001525956 T	11-12-2001
		JP 2001527674 T	25-12-2001
		JP 2002512715 T	23-04-2002
		JP 2001527675 T	25-12-2001
		JP 2001525958 T	11-12-2001
		US 6575372 B1	10-06-2003
		US 2002050528 A1	02-05-2002
		US 6220510 B1	24-04-2001
		US 6230267 B1	08-05-2001
		US 6164549 A	26-12-2000
		US 6488211 B1	03-12-2002
		US 6317832 B1	13-11-2001
		US 6328217 B1	11-12-2001
		US 2003024980 A1	06-02-2003
EP 0973135 A	19-01-2000	JP 2000036014 A	02-02-2000
		EP 0973135 A2	19-01-2000
		KR 2000011792 A	25-02-2000
		SG 94329 A1	18-02-2003
		TW 475126 B	01-02-2002
US 5577121 A	19-11-1996	US 5892211 A	06-04-1999

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2004/051198

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0127886 A	19-04-2001	FI 992197 A	30-04-2001
		AU 7792900 A	23-04-2001
		CN 1139902 C	25-02-2004
		EP 1242981 A1	25-09-2002
		WO 0127886 A1	19-04-2001
US 2002050528 A1	02-05-2002	US 6575372 B1	10-06-2003
		AU 736325 B2	26-07-2001
		AU 6299698 A	09-09-1998
		CA 2281576 A1	27-08-1998
		DE 69823649 D1	09-06-2004
		EP 0963580 A1	15-12-1999
		WO 9837526 A1	27-08-1998
		JP 2001513231 T	28-08-2001
		ZA 9801422 A	24-08-1998
		AU 7777298 A	08-12-1998
		DE 69807210 D1	19-09-2002
		DE 69807210 T2	24-04-2003
		EP 0976114 A2	02-02-2000
		WO 9852162 A2	19-11-1998
		HK 1022364 A1	02-05-2003
		JP 2002512715 T	23-04-2002
		US 6317832 B1	13-11-2001
		US 2001056536 A1	27-12-2001
		AU 7776798 A	08-12-1998
		AU 7776898 A	08-12-1998
		AU 7776998 A	08-12-1998
		AU 7777098 A	08-12-1998
		AU 7777198 A	08-12-1998
		AU 7777398 A	08-12-1998
		AU 7777498 A	08-12-1998
		DE 69813208 D1	15-05-2003
		DE 69813208 T2	05-02-2004
		EP 0981807 A2	01-03-2000
		EP 0985202 A1	15-03-2000
		EP 0985203 A1	15-03-2000
		EP 0985204 A1	15-03-2000
		EP 0981805 A1	01-03-2000
		WO 9852158 A2	19-11-1998
		WO 9852159 A2	19-11-1998
		WO 9852160 A2	19-11-1998
		WO 9852161 A2	19-11-1998
		WO 9852152 A2	19-11-1998
		WO 9852163 A2	19-11-1998
		WO 9852153 A2	19-11-1998
		JP 2001525956 T	11-12-2001
		JP 2001527674 T	25-12-2001
		JP 2001525957 T	11-12-2001
		JP 2001527675 T	25-12-2001
		JP 2001525958 T	11-12-2001
		US 6220510 B1	24-04-2001
		US 6230267 B1	08-05-2001
		US 6385723 B1	07-05-2002
		US 6164549 A	26-12-2000
		US 6488211 B1	03-12-2002

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/EP2004/051198

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	US 6 385 723 B1 (RICHARDS TIMOTHY PHILIP) 7 mai 2002 (2002-05-07) colonne 4, ligne 10 - colonne 12, ligne 16 figure 1	1-9
Y	EP 0 973 135 A (SONY CORP) 19 janvier 2000 (2000-01-19) colonne 12, alinéa 78 - colonne 13, alinéa 87 colonne 16, alinéa 105 - colonne 17, alinéa 110 colonne 19, alinéa 125 - alinéa 126 figure 7	1-9
A	US 5 577 121 A (DAVIS TERRY L ET AL) 19 novembre 1996 (1996-11-19) abrégé	2

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
20 août 2004	30/08/2004

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Rachkov, V

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/EP2004/051198

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	BRUCE SCHNEIER: "Applied Cryptography" 1996, JOHN WILEY & SONS, INC. , USA 238530 , XP002267052 page 513 - page 514	3,4,6,7
A	WO 01/27886 A (HAEMAELAEINEN ANTTI ;SONERA SMARTTRUST OY (FI)) 19 avril 2001 (2001-04-19) page 6, ligne 1 - page 13, ligne 7 figure 3	1
A	US 2002/050528 A1 (MILLER STUART JAMES ET AL) 2 mai 2002 (2002-05-02) page 1, alinéa 6 page 2, alinéa 25 - page 3, alinéa 32 page 5, alinéa 55 - page 8, alinéa 82 figure 10	1-9

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/EP2004/051198

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 6385723 B1	07-05-2002	AU 7777098 A	08-12-1998
		EP 0985203 A1	15-03-2000
		WO 9852161 A2	19-11-1998
		JP 2001525957 T	11-12-2001
		AU 736325 B2	26-07-2001
		AU 6299698 A	09-09-1998
		AU 7776798 A	08-12-1998
		AU 7776898 A	08-12-1998
		AU 7776998 A	08-12-1998
		AU 7777198 A	08-12-1998
		AU 7777298 A	08-12-1998
		AU 7777398 A	08-12-1998
		AU 7777498 A	08-12-1998
		CA 2281576 A1	27-08-1998
		DE 69807210 D1	19-09-2002
		DE 69807210 T2	24-04-2003
		DE 69813208 D1	15-05-2003
		DE 69813208 T2	05-02-2004
		DE 69823649 D1	09-06-2004
		EP 0963580 A1	15-12-1999
		EP 0981807 A2	01-03-2000
		EP 0985202 A1	15-03-2000
		EP 0976114 A2	02-02-2000
		EP 0985204 A1	15-03-2000
		EP 0981805 A1	01-03-2000
		WO 9837526 A1	27-08-1998
		WO 9852158 A2	19-11-1998
		WO 9852159 A2	19-11-1998
		WO 9852160 A2	19-11-1998
		WO 9852152 A2	19-11-1998
		WO 9852162 A2	19-11-1998
		WO 9852163 A2	19-11-1998
		WO 9852153 A2	19-11-1998
		HK 1022364 A1	02-05-2003
		JP 2001513231 T	28-08-2001
		JP 2001525956 T	11-12-2001
		JP 2001527674 T	25-12-2001
		JP 2002512715 T	23-04-2002
		JP 2001527675 T	25-12-2001
		JP 2001525958 T	11-12-2001
		US 6575372 B1	10-06-2003
		US 2002050528 A1	02-05-2002
		US 6220510 B1	24-04-2001
		US 6230267 B1	08-05-2001
		US 6164549 A	26-12-2000
		US 6488211 B1	03-12-2002
		US 6317832 B1	13-11-2001
		US 6328217 B1	11-12-2001
		US 2003024980 A1	06-02-2003
EP 0973135 A	19-01-2000	JP 2000036014 A	02-02-2000
		EP 0973135 A2	19-01-2000
		KR 2000011792 A	25-02-2000
		SG 94329 A1	18-02-2003
		TW 475126 B	01-02-2002
US 5577121 A	19-11-1996	US 5892211 A	06-04-1999

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/EP2004/051198

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 0127886 A	19-04-2001	FI 992197 A	30-04-2001
		AU 7792900 A	23-04-2001
		CN 1139902 C	25-02-2004
		EP 1242981 A1	25-09-2002
		WO 0127886 A1	19-04-2001
US 2002050528 A1	02-05-2002	US 6575372 B1	10-06-2003
		AU 736325 B2	26-07-2001
		AU 6299698 A	09-09-1998
		CA 2281576 A1	27-08-1998
		DE 69823649 D1	09-06-2004
		EP 0963580 A1	15-12-1999
		WO 9837526 A1	27-08-1998
		JP 2001513231 T	28-08-2001
		ZA 9801422 A	24-08-1998
		AU 7777298 A	08-12-1998
		DE 69807210 D1	19-09-2002
		DE 69807210 T2	24-04-2003
		EP 0976114 A2	02-02-2000
		WO 9852162 A2	19-11-1998
		HK 1022364 A1	02-05-2003
		JP 2002512715 T	23-04-2002
		US 6317832 B1	13-11-2001
		US 2001056536 A1	27-12-2001
		AU 7776798 A	08-12-1998
		AU 7776898 A	08-12-1998
		AU 7776998 A	08-12-1998
		AU 7777098 A	08-12-1998
		AU 7777198 A	08-12-1998
		AU 7777398 A	08-12-1998
		AU 7777498 A	08-12-1998
		DE 69813208 D1	15-05-2003
		DE 69813208 T2	05-02-2004
		EP 0981807 A2	01-03-2000
		EP 0985202 A1	15-03-2000
		EP 0985203 A1	15-03-2000
		EP 0985204 A1	15-03-2000
		EP 0981805 A1	01-03-2000
		WO 9852158 A2	19-11-1998
		WO 9852159 A2	19-11-1998
		WO 9852160 A2	19-11-1998
		WO 9852161 A2	19-11-1998
		WO 9852152 A2	19-11-1998
		WO 9852163 A2	19-11-1998
		WO 9852153 A2	19-11-1998
		JP 2001525956 T	11-12-2001
		JP 2001527674 T	25-12-2001
		JP 2001525957 T	11-12-2001
		JP 2001527675 T	25-12-2001
		JP 2001525958 T	11-12-2001
		US 6220510 B1	24-04-2001
		US 6230267 B1	08-05-2001
		US 6385723 B1	07-05-2002
		US 6164549 A	26-12-2000
		US 6488211 B1	03-12-2002